

**LAPORAN PRAKTIKUM**  
**KEAMANAN INFORMASI 1**  
**PERTEMUAN 8**  
*(Crafting dan DNS Recon)*



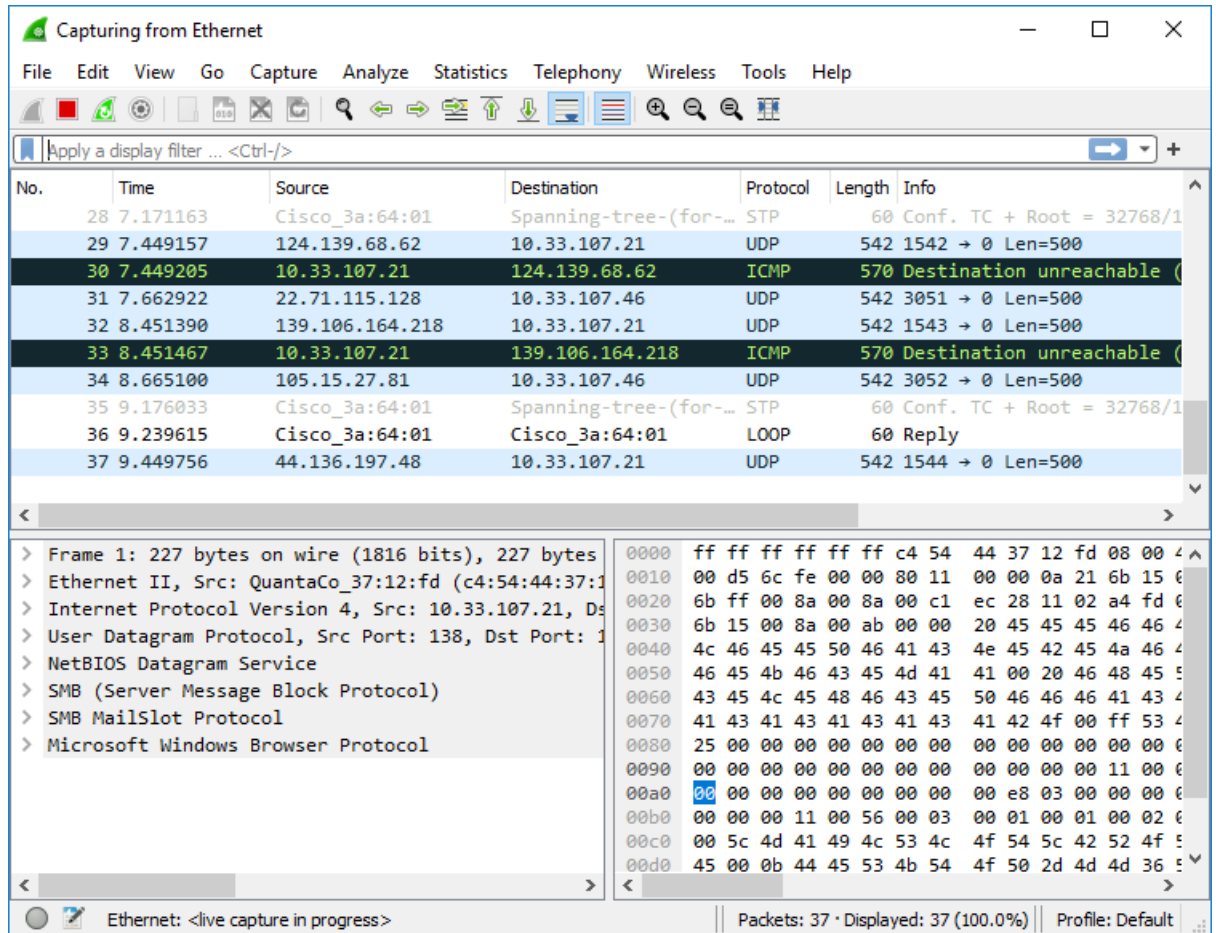
**DISUSUN OLEH**

Indah Sekar Ningrum      (21/478139/SV/19241)

**SARJANA TERAPAN TEKNOLOGI REKAYASA INTERNET**  
**DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA**  
**SEKOLAH VOKASI**  
**UNIVERSITAS GADJAH MADA**  
**YOGYAKARTA**

**2023**

## 1. Wireshark ethernet



## 2. Hping3 -c 3 10.33.107.21

```
(root@kali)~# hping3 -c 3 10.33.107.21
HPING 10.33.107.21 (eth0 10.33.107.21): NO FLAGS are set, 40 headers + 0 data bytes
len=46 ip=10.33.107.21 ttl=127 DF id=19332 sport=0 flags=RA seq=0 win=0 rtt=7.9 ms
len=46 ip=10.33.107.21 ttl=127 DF id=19343 sport=0 flags=RA seq=1 win=0 rtt=7.7 ms
len=46 ip=10.33.107.21 ttl=127 DF id=19353 sport=0 flags=RA seq=2 win=0 rtt=7.5 ms

--- 10.33.107.21 hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 7.5/7.7/7.9 ms
```

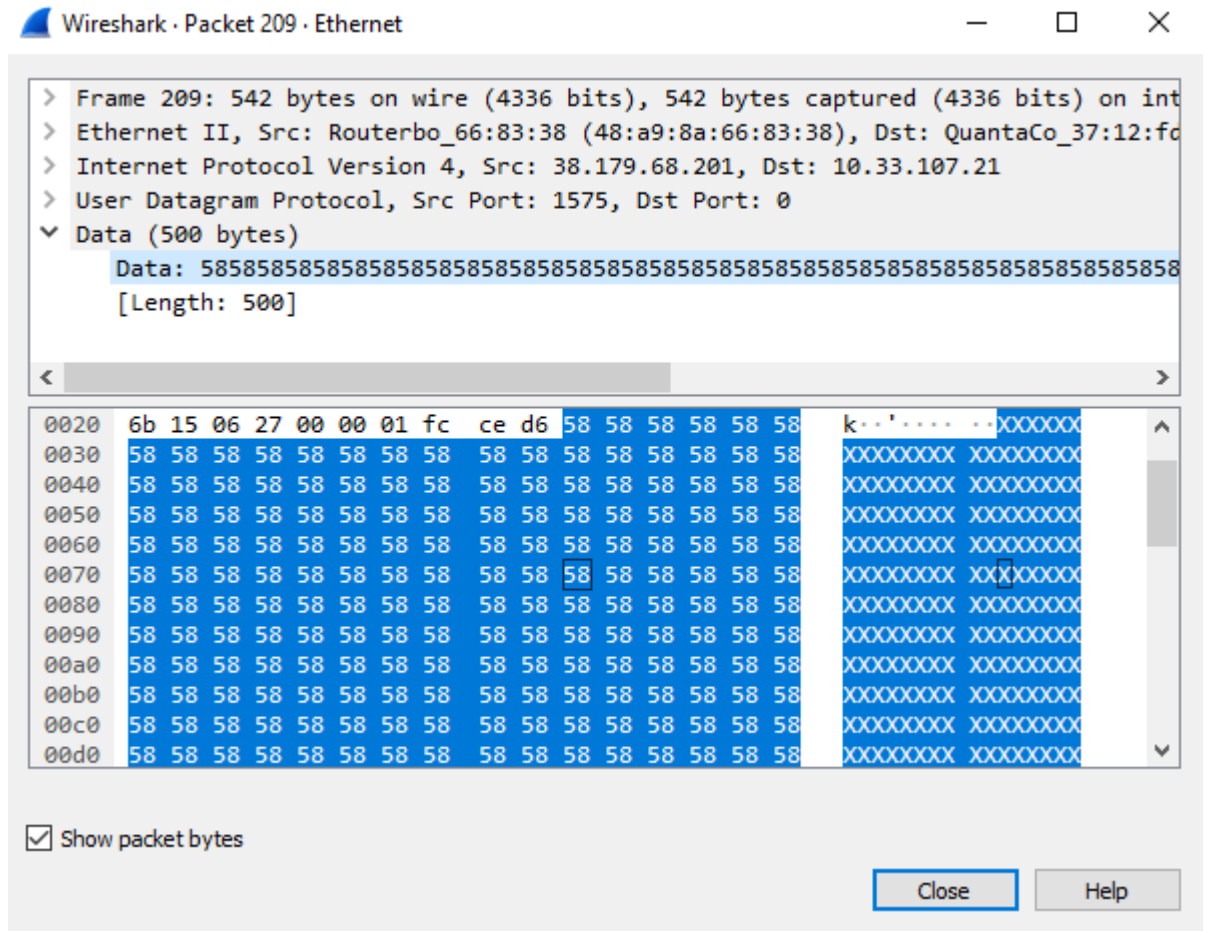
## 3. Hping3 --scan 1-3000 -S 10.33.107.21

```
(root@kali)~# hping3 --scan 1-3000 -S 10.33.107.21
Scanning 10.33.107.21 (10.33.107.21), port 1-3000
3000 ports to scan, use -V to see all the replies
+---+---+---+---+---+---+
|port| serv name | flags |ttl| id | win | len |
+---+---+---+---+---+---+
1521 : .S..A... 127 44895 65392 46
135 epmap : .S..A... 127 57951 65392 46
139 netbios-ssn: .S..A... 127 33376 8192 46
445 microsoft-d: .S..A... 127 47456 65392 46
2030 : .S..A... 127 6243 65392 46
All replies received. Done.
```

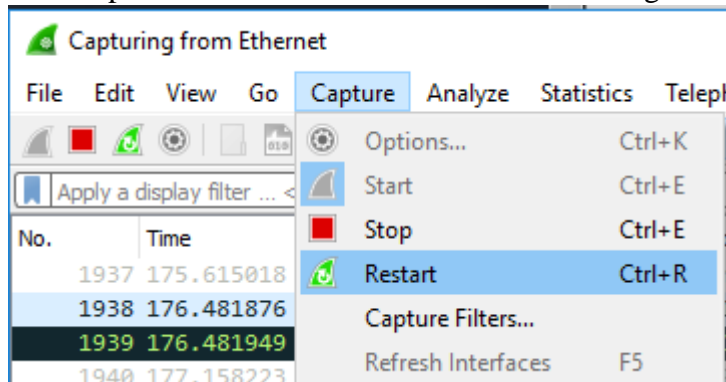
4. Hping3 10.33.107.21 --udp --rand-source --data 500

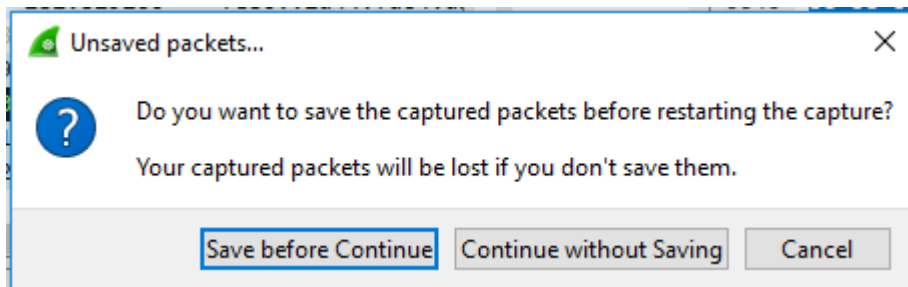
```
(root@kali)~# hping3 10.33.107.21 --udp --rand-source --data 500
HPING 10.33.107.21 (eth0 10.33.107.21): udp mode set, 28 headers + 500 data bytes
```

5. Wireshark UDP



6. Klik Capture > Restart > Continue Without Saving



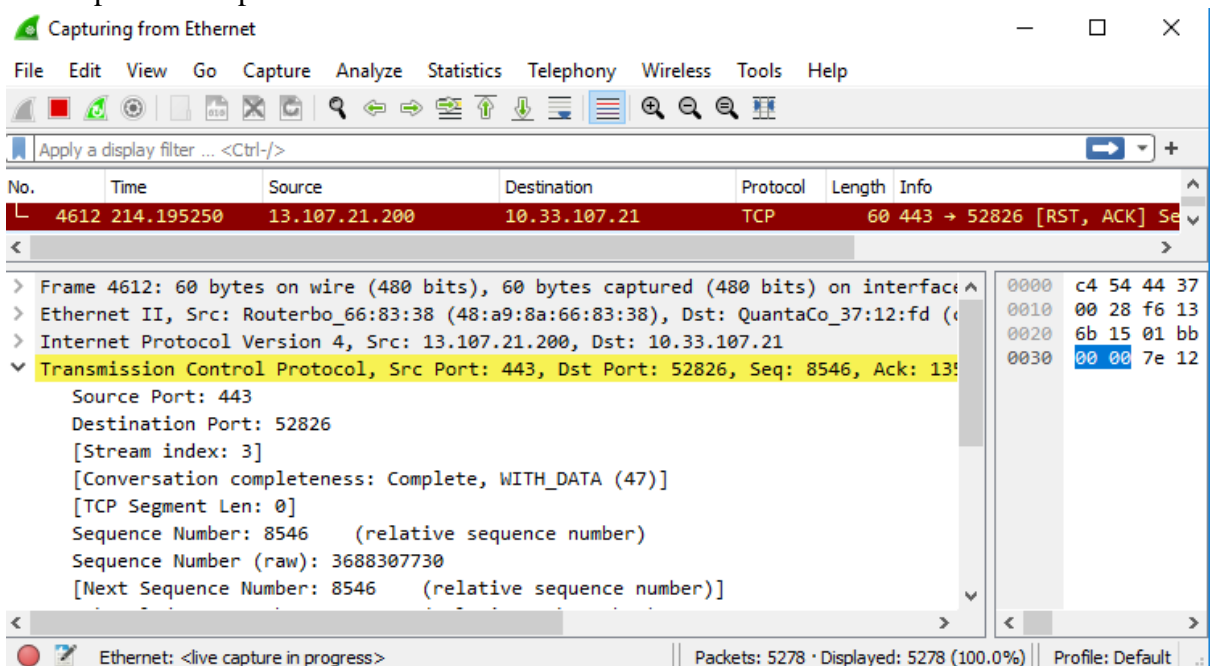


7. Hping3 -S 10.33.107.21 -p 80 -c 5

```
(root@kali)~[/home/kali]
# hping3 -S 10.33.107.21 -p 80 -c 5
HPING 10.33.107.21 (eth0 10.33.107.21): S set, 40 headers + 0 data bytes
len=46 ip=10.33.107.21 ttl=127 DF id=6988 sport=80 flags=RA seq=0 win=0 rtt=3.5 ms
len=46 ip=10.33.107.21 ttl=127 DF id=6988 sport=80 flags=RA seq=1 win=0 rtt=3.3 ms
len=46 ip=10.33.107.21 ttl=127 DF id=7004 sport=80 flags=RA seq=2 win=0 rtt=3.1 ms
len=46 ip=10.33.107.21 ttl=127 DF id=7012 sport=80 flags=RA seq=3 win=0 rtt=6.9 ms
len=46 ip=10.33.107.21 ttl=127 DF id=7022 sport=80 flags=RA seq=4 win=0 rtt=6.7 ms

--- 10.33.107.21 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 3.1/4.7/6.9 ms
```

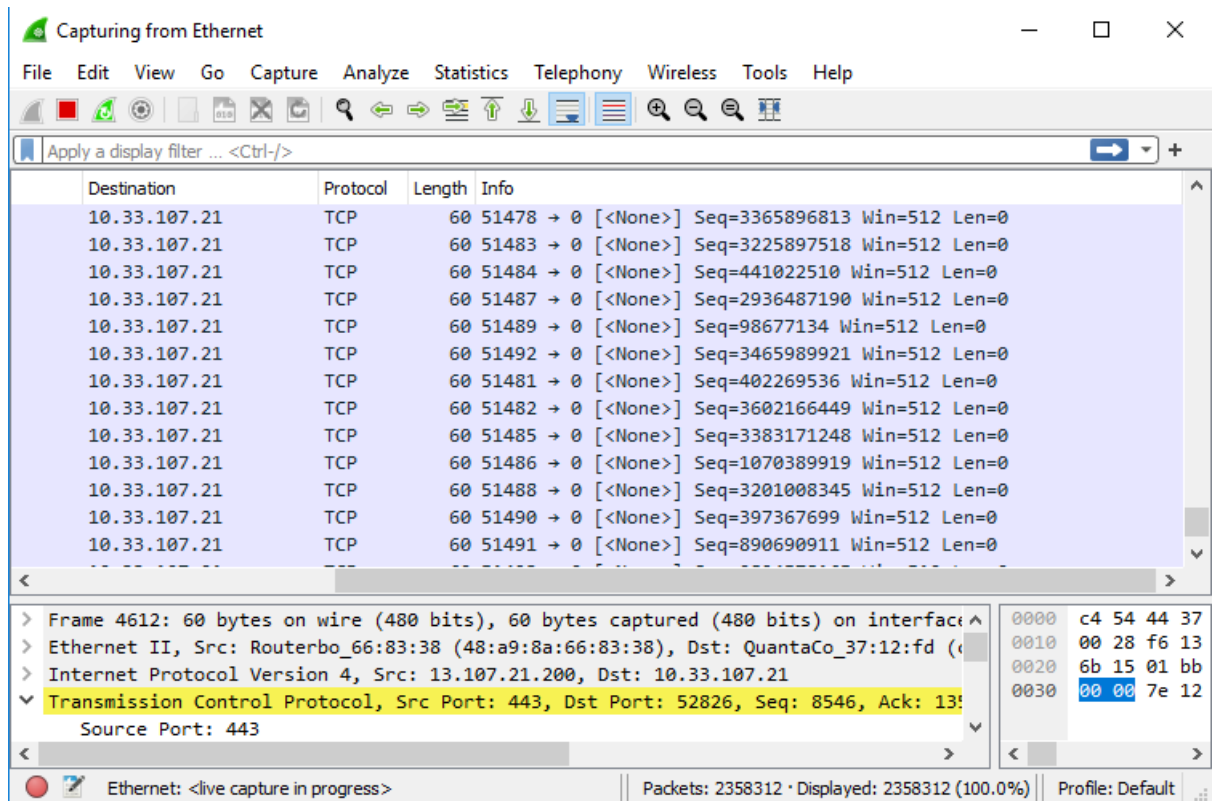
8. Amati paket TCP pada Wireshark



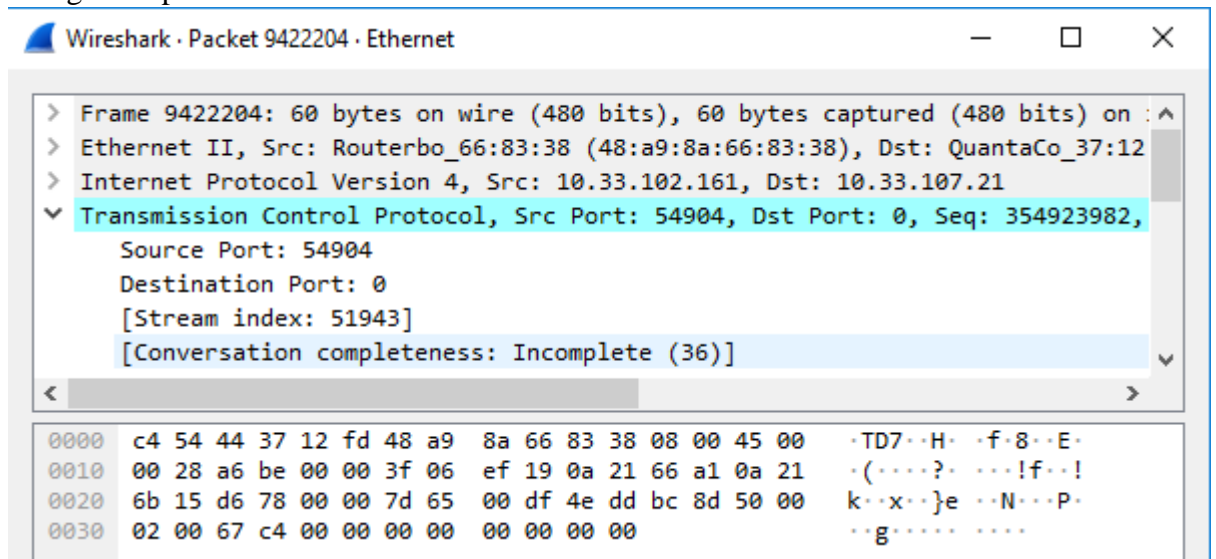
9. Hping3 10.33.107.21 --flood

```
(root@kali)~[/home/kali]
# hping3 10.33.107.21 --flood
HPING 10.33.107.21 (eth0 10.33.107.21): NO FLAGS are set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

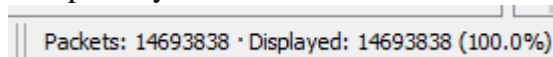
10. TCP membanjir



## 11. Mengamati paket TCP



## 12. Berapa banyak





1. Dnsrecon -d [www.acme.com](http://www.acme.com)

```
(root@kali)~[/home/kali]
# dnsrecon -d www.acme.com
[*] Performing General Enumeration of Domain: www.acme.com
[-] DNSSEC is not configured for www.acme.com
[*] NS dns2.name-services.com 216.40.47.201
[*] NS dns2.name-services.com 2604:4000:0:d:216:40:47:201
[*] NS dns5.name-services.com 64.98.148.139
[*] NS dns5.name-services.com 2604:4000:2800:2000:64:98:148:139
[*] NS dns3.name-services.com 64.98.148.138
[*] NS dns3.name-services.com 2604:4000:2800:2000:64:98:148:138
[*] NS dns1.name-services.com 64.98.148.137
[*] NS dns1.name-services.com 2604:4000:2800:2000:64:98:148:137
[*] NS dns4.name-services.com 216.40.47.202
[*] NS dns4.name-services.com 2604:4000:0:d:216:40:47:202
[-] Could not Resolve MX Records for www.acme.com
[*] CNAME www.acme.com acme.com
[*] A acme.com 23.93.76.124
[*] Enumerating SRV Records
[+] 0 Records Found
```

2. Dnsrecon -d [www.certifiedhacker.com](http://www.certifiedhacker.com)

```
(root@kali)~[/home/kali]
# dnsrecon -d www.certifiedhacker.com
[*] Performing General Enumeration of Domain: www.certifiedhacker.com
[-] DNSSEC is not configured for www.certifiedhacker.com
[*] NS ns2.bluehost.com 162.159.25.175
[*] NS ns1.bluehost.com 162.159.24.80
[*] MX mail.certifiedhacker.com 162.241.216.11
[*] CNAME www.certifiedhacker.com certifiedhacker.com
[*] A certifiedhacker.com 162.241.216.11
[*] TXT www.certifiedhacker.com v=spf1 a mx ptr include:bluehost.com ?all
[*] Enumerating SRV Records
[+] 0 Records Found
```

3. Dnsrecon -t snoop -n ns\_server -d [www.acme.com](http://www.acme.com) -D /path/to/dict.txt

```
(root@kali)~[/home/kali]
# dnsrecon -t snoop -n ns_server -d www.acme.com -D /path/to/dict.txt
[-] Could not resolve NS server provided and server doesn't appear to be an IP: ns_server
[-] Please specify valid name servers.
```

4. Dnsrecon -d [www.acme.com](http://www.acme.com) -t zonewalk

```
(root@kali)~[/home/kali]
# dnsrecon -d www.acme.com -t zonewalk
[*] Performing NSEC Zone Walk for www.acme.com
[*] Getting SOA record for www.acme.com
[-] This zone appears to be misconfigured, no SOA record found.
[*] CNAME www.acme.com acme.com
[*] A acme.com 23.93.76.124
[+] 2 records found
```

5. Dnsrecon -d [www.acme.com](http://www.acme.com) -D /path/to/dict.txt -t brt

```
(root@kali)~[/home/kali]
# dnsrecon -d www.acme.com -D /path/to/dict.txt -t brt
[-] File /path/to/dict.txt does not exist!
```

6. Dnsrecon -d [www.acme.com](http://www.acme.com) -t axfr

```

(root@kali)-[/home/kali]
# dnsrecon -d www.acme.com -t axfr
[*] Testing NS Servers for Zone Transfer
[*] Checking for Zone Transfer for www.acme.com name servers
[*] Resolving SOA Record
[*] Resolving NS Records
[*] NS Servers found:
[*] NS dns3.name-services.com 64.98.148.138
[*] NS dns3.name-services.com 2604:4000:2800:2000:64:98:148:138
[*] NS dns5.name-services.com 64.98.148.139
[*] NS dns5.name-services.com 2604:4000:2800:2000:64:98:148:139
[*] NS dns1.name-services.com 64.98.148.137
[*] NS dns1.name-services.com 2604:4000:2800:2000:64:98:148:137
[*] NS dns2.name-services.com 216.40.47.201
[*] NS dns2.name-services.com 2604:4000:0:d:216:40:47:201
[*] NS dns4.name-services.com 216.40.47.202
[*] NS dns4.name-services.com 2604:4000:0:d:216:40:47:202
[*] Removing any duplicate NS server IP Addresses ...
[*]
[*] Trying NS server 2604:4000:2800:2000:64:98:148:137
[-] Zone Transfer Failed for 2604:4000:2800:2000:64:98:148:137!
[-] Port 53 TCP is being filtered
[*]
[*] Trying NS server 216.40.47.201
[-] Zone Transfer Failed for 216.40.47.201!
[-] Port 53 TCP is being filtered
[*]
[*] Trying NS server 2604:4000:2800:2000:64:98:148:139
[-] Zone Transfer Failed for 2604:4000:2800:2000:64:98:148:139!
[-] Port 53 TCP is being filtered
[*]
[*] Trying NS server 64.98.148.137
[-] Zone Transfer Failed for 64.98.148.137!
[-] Port 53 TCP is being filtered
[*]
[*] Trying NS server 64.98.148.139
[-] Zone Transfer Failed for 64.98.148.139!
[-] Port 53 TCP is being filtered
[*]
[*] Trying NS server 2604:4000:2800:2000:64:98:148:138
[-] Zone Transfer Failed for 2604:4000:2800:2000:64:98:148:138!
[-] Port 53 TCP is being filtered
[*]

```

7. Dnsrecon -r 208.67.222.200-208.67.222.255 -d microsoft.com

```

(root@kali)-[/home/kali]
# dnsrecon -r 208.67.222.200-208.67.222.255 -d microsoft.com
[*] Reverse Look-up of a Range
[*] Performing Reverse Lookup from 208.67.222.200 to 208.67.222.255
[+] PTR resolver3.opendns.com 208.67.222.220
[+] PTR dns.umbrella.com 208.67.222.222
[+] PTR dns.opendns.com 208.67.222.222
[+] PTR resolver1.opendns.com 208.67.222.222
[+] 4 Records Found

```